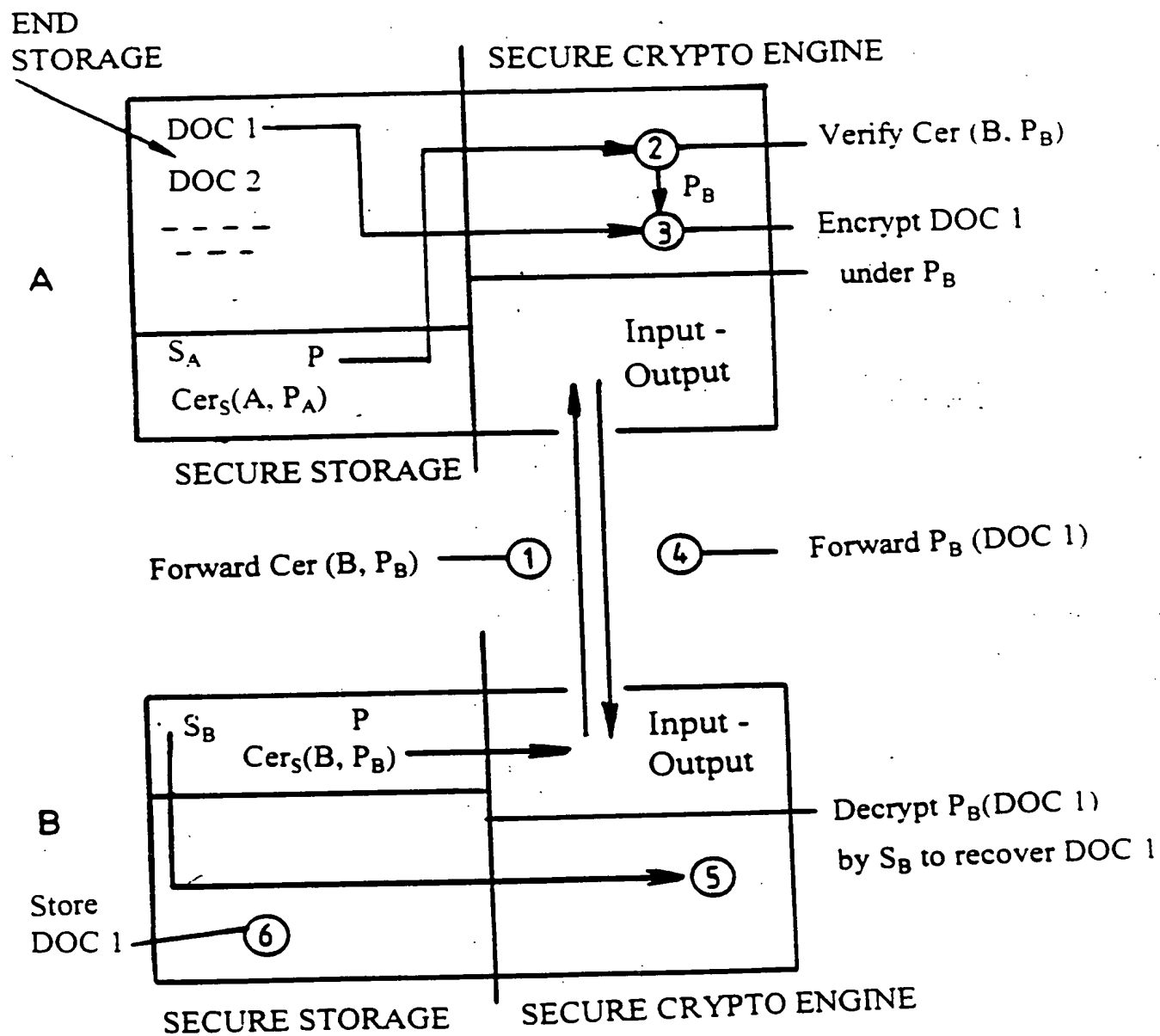


FIG. 1



P: Public key of CA

S: Secret key of CA

FIG.2END Generation

CREATE CONTENT	END
↓	
ADD TIMESTAMP	END + T → STORE
↓	
CALCULATE HASH	$h(\text{END} + T) = h_1$
↓	
INPUT D-C	{ END OUTSIDE $h_1$ INSIDE
↓	
APPEND DEVICE NO.	$D(j)$
↓	
APPEND SEQ. NO.	$S(i)$
↓	
(APPEND WM = IDENTIFICATION)	
↓	
CALCULATE HASH	$h(h_1 + D(j) + S(i) + \text{WM}) = h_2$
↓	
SIGN HASH	$S_j(h_2)$
↓	
STORE	$h(h_1 + D(j) + S(i) + \text{WM}), S_j(h_2)$
↓	
APPEND COUNTER = "0", FLAG = "1" (SELL)	

FIG.3NEGOTIATION.

Stage	SELLER, using D-C <sub>A</sub>		BUYER, using D-C <sub>B</sub>
1		←	Send public key P <sub>B</sub> cert. C <sub>B</sub>
2	Verify Certificate C <sub>B</sub>	by D-C <sub>A</sub>	
3	Specify D(j), S(i)	input	
4	Verify flag = 1	by D-C <sub>A</sub>	
5	Encrypt specified END record M under P <sub>B</sub> to generate ciphertext C		
6	Set flag = 0, send C, END and certificate of Issuer (j)	→	
7		by D-C <sub>B</sub>	Decrypt C
8		by D-C <sub>B</sub>	Verify issuer's signature
9		by owner	Check validity period
10			Store in new END record
11			Increment counter, set flag = 1